PCT/JP99/00533

09/403071

日本国特許庁

08.02.99

PATENT OFFICE
JAPANESE GOVERNMENT

E.U.

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　２月１３日

出願番号
Application Number: 平成１０年特許願第０３１８４７号

出願人
Applicant (s): 松下電器産業株式会社

１９９９年　３月１２日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

出証番号　出証特平１１－３０１３０２５

【書類名】　特許願

【整理番号】　2054001030

【提出日】　平成10年 2月13日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明の名称】　デジタルＡＶデータ送信ユニット、デジタルＡＶデータ受信ユニット及び、デジタルＡＶデータ送受信システム、媒体

【請求項の数】　17

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　飯塚　裕之

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山田　正純

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　武知　秀明

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　臼木　直司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　後藤　昌一

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100092794

【弁理士】

【氏名又は名称】　松田　正道

【電話番号】　06 397-2840

【手数料の表示】

【予納台帳番号】　009896

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9006027

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デジタルＡＶデータ送信ユニット、デジタルＡＶデータ受信ユニット及び、デジタルＡＶデータ送受信システム、媒体

【特許請求の範囲】

【請求項１】　デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項２】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項３】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と

同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項４】　デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項５】　前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項３記載のデジタルAVデータ送受信システム。

【請求項６】　前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項５記載のデジタルAVデータ送受信システム。

【請求項７】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニット。

【請求項８】　複数種類の認証ルールを格納した送信側複数認証ルール格納手

段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニット。

【請求項９】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１０】　所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決

定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶ送信ユニット。

【請求項１１】　前記管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）であることを特徴とする請求項４又は１０に記載のデジタルＡＶ送信ユニット。

【請求項１２】前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルＡＶデータをやりとりできることを特徴とする請求項９記載のデジタルＡＶデータ送受信システム。

【請求項１３】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項１４】　複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認

証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、

認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルＡＶデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１５】前記複数認証デジタルＡＶデータ受信ユニットは前記デジタルＡＶデータ送信ユニットの各機能を有し、前記デジタルＡＶデータ送信ユニットは前記複数認証デジタルＡＶデータ受信ユニットの各機能を有することを特徴とする請求項１４記載のデジタルＡＶデータ送受信システム。

【請求項１６】前記複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいは前記デジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項１５記載のデジタルＡＶデータ送受信システム。

【請求項１７】請求項１～１６のいずれかに記載のユニット又はシステムが有する各構成要素が持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＡＶ装置間において認証を行う機能を持つＡＶシステムに関するものである。

【０００２】

【従来の技術】

従来のＡＶ装置間において認証を行うシステムについて図２と図３を用いて説明する。

【０００３】

まず、図２において、デジタルＡＶデータ送信ユニットＳＴＢ１８は、公開鍵と秘密鍵２０、認証手段１９、デジタルインターフェースＤ－Ｉ／Ｆ２２、暗号化手段１９を備えている。その公開鍵と秘密鍵２０は、認証手段１９を介して、デジタルインターフェースＤ－Ｉ／Ｆ２２に接続している。また、暗号化手段１９は、公開鍵と秘密鍵２０を参照することが出来、デジタルインターフェース２２に接続している。デジタルＡＶデータ受信ユニットＴＶ２３も公開鍵と秘密鍵２６、認証手段２５、デジタルインターフェースＤ－Ｉ／Ｆ２４、復号化手段２７を具備している。その公開鍵と秘密鍵２６は認証手段２５を介してデジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。また、復号化手段２７は公開鍵と秘密鍵２６を参照することが出来、デジタルインターフェースＤ－Ｉ／Ｆ２４に接続している。さらにデジタルインターフェースＤ－Ｉ／Ｆ２２とデジタルインターフェースＤ－Ｉ／Ｆ２４は互いにデータのやり取りが出来る構成となっている。

【０００４】

次にデジタルＡＶデータ送信ユニットＳＴＢ１８とデジタルＡＶデータ受信ユニットＴＶ２３間の動作を説明する。まず、デジタルＡＶデータ受信ユニットＴＶ２３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ２４を通してデジタルＡＶデータ送信ユニットＳＴＢ１８を構成するデジタルインターフェースＤ－Ｉ／Ｆ２２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ２２は認証要求を受けて認証手段１９にて、公開鍵と秘密鍵２０を参照して認証する。デジタルＡＶデータ送信ユニットＳＴＢ１８にて認証されれば、暗号

化手段２１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ２２を介して、暗号化したデータが送信される。これはデジタルインターフェースＤ－Ｉ／Ｆ２４を介して、公開鍵と秘密鍵２６を参照して、復号化手段２７で復号される。

【０００５】

このようにすると、偽造や改竄に強い機能が実現出来る。しかし、公開鍵と秘密鍵を用いた認証は多くの時間を要する。ニュースのように、あまり重要でないデータの場合、不必要に認証に時間を取られることがある。またＶＴＲのようにコピー可能なデータしか受け取っては機器は、場合によってデジタルＡＶデータ受信ユニットが厳密な認証を要しないこともあり、そのような場合、時間の無駄が生じる。

【０００６】

次に、図３において、デジタルＡＶ送信ユニットＳＴＢ２８は共通鍵３０、認証手段２９、デジタルインターフェースＤ－Ｉ／Ｆ３２、暗号化手段３１を具備している。その共通鍵３０は、認証手段２９を介して、デジタルインターフェースＤ－Ｉ／Ｆ３２に接続している。また、暗号化手段３１は、共通鍵３０を参照することが出来、デジタルインターフェース３２に接続している。デジタルＡＶデータ受信ユニットＴＶ３３も、共通鍵３６、認証手段３５、デジタルインターフェース３４、復号化手段３７を具備している。その共通鍵３６は認証手段３５を介してデジタルインターフェース３４に接続している。また、復号化手段３７は共通鍵３６を参照することが出来、デジタルインターフェース３４に接続している。さらにデジタルインターフェース３２とデジタルインターフェース３４は互いにデータのやり取りが出来る構成となっている。

【０００７】

次にデジタルＡＶデータ送信ユニットＳＴＢ２８とデジタルＡＶデータ受信ユニットＴＶ３３間の動作を説明する。まず、デジタルＡＶ受信ユニットＴＶ３３が認証要求を出す。するとデジタルインターフェースＤ－Ｉ／Ｆ３４を通してデジタルＡＶ送信ユニットＳＴＢ２８を構成するデジタルインターフェースＤ－Ｉ／Ｆ３２に認証要求が到達する。デジタルインターフェースＤ－Ｉ／Ｆ３２は認

証要求を受けて認証手段２９にて、共通鍵３０を参照して認証する。デジタルＡＶ送信ユニットＳＴＢ２８にて認証されれば、暗号化手段３１において、データが暗号化されて、デジタルインターフェースＤ－Ｉ／Ｆ３２を介して、暗号化したデータが送信される。これはデジタルインターフェースD－I／Ｆ３４を介して、共通鍵３６を参照してデジタ復号化手段３７で復号される。

【０００８】

このようにすると、短い時間でデータの認証を行うことができる。しかし、共通鍵を用いた認証は偽造や改竄に弱いので、新作の映画など著作権上重要なデータの場合、第三者にデータを無料で視聴されることがある。またＴＶのように受信した全てのデータを表示するために、厳密な認証を行う機器と接続した場合に対応できる必要があり、デジタルAVデータ受信ユニットが厳密な認証を要する場合があり、そのような場合重要なデータの著作権が保護されないといったことが起こりうる。

【０００９】

【発明が解決しようとする課題】

このように、あまり重要でないデータの認証に多くの時間を要するという課題や、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題が存在する。また、デジタルＡＶデータ受信ユニットによっては、厳密な認証を要しないものも存在し、このようなユニットに対して厳密な認証を行った場合、時間の無駄が生じるという課題や、逆にデジタルＡＶデータ受信ユニットによっては厳密な認証を要するものも存在し、そのようなユニットに厳密でない認証を行った場合、著作権が守られないといった課題が存在する。

【００１０】

本発明は、このような従来の、重要でないデータの認証に多くの時間を要するという課題と、重要なデータであるにもかかわらずそのの認証が偽造や改竄に弱いという課題と、ユニットによって認証に必要な厳密さが異なるといった課題を考慮し、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、システム等を提供することを目的とするものである。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニットである。

【００１２】

また請求項２の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニットである。

【００１３】

また請求項３の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルＡＶデータ受信ユニットとを備えたことを特徴とするデジタルＡＶデータ送受信システムである。

【００１４】

また請求項４の本発明は、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基き、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニットである。

【００１５】

また請求項５の本発明は、前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項３記載のデジタルＡＶデータ送受信システムである。

【００１６】

また請求項６の本発明は、前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項５記載のデジタルＡＶデータ送受信システムである。

【００１７】

また請求項７の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認

証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルＡＶ送信ユニットである。

【００１８】

また請求項８の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットを通信の対象とし、

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ受信ユニットである。

【００１９】

また請求項９の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと

前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納

する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システムである。

【００２０】

また請求項１０の本発明は、所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶ送信ユニットである。

【００２１】

また請求項１１の本発明は、前記管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）であることを特徴とする請求項４又は１０に記載のデジタルＡＶ送信ユニットである。

【００２２】

また請求項１２の本発明は、前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルＡＶデータをやりとりできることを特徴とする請求項９記載のデジタルＡＶデータ送受信システムである。

【００２３】

また請求項１３の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタ

ルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニットである。

【００２４】

また請求項１４の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、

認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルＡＶデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システムである。

【００２５】

また請求項１５の本発明は、前記複数認証デジタルＡＶデータ受信ユニットは前記デジタルＡＶデータ送信ユニットの各機能を有し、前記デジタルＡＶデータ送信ユニットは前記複数認証デジタルＡＶデータ受信ユニットの各機能を有することを特徴とする請求項１４記載のデジタルＡＶデータ送受信システムである。

【００２６】

また請求項１６の本発明は前記複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいは前記デジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項１５記載のデジタルＡＶデータ送受信システムである。

【００２７】

また、請求項１７の本発明は、請求項１～１６のいずれかに記載のユニット又はシステムが有する各構成要素が持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体である。

【００２８】

【発明の実施の形態】

以下に本発明の実施の形態を図面を参照して説明する。

【００２９】

まず、第一の実施の形態について図1を参照して説明する。

【００３０】

デジタルＡＶデータ送信ユニットＳＴＢ１は、データ重要性判定手段３、暗号化手段４、送信側複数認証ルール格納手段５、送信側認証選択手段６、送信側認証手段７及びデジタルインターフェースＤ－Ｉ／Ｆ８を持つ。このデータ重要性判定手段３は、データ２の重要性を重要度に応じて複数種類に場合分けを行う手段である。このデータの重要度はＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段４は、データ２を、認証の過程で作成されたワーク鍵Ｋｗ１６で暗号化する手

段である。ワーク鍵Ｋｗ１６を生成するその認証方法は後述する。送信側複数認証ルール格納手段５は、複数種類の認証ルールを持つ手段である。例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールの２種類の認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段６は、送信側複数認証ルール格納手段５が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この際、データ重要性判定手段３の判定の結果を参考にする。本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱いルールとして、共通鍵を用いた認証ルールを選択する。送信側認証手段７は、選択された認証ルールで実際にデジタルＡＶデータ受信ユニットＴＶ９と認証をかわす手段である。デジタルインターフェースＤ－Ｉ／Ｆ８は、デジタルＡＶデータ受信ユニットＴＶ９とＡＶデータや信号のやりとりを行う手段である。

【００３１】

デジタルＡＶデータ受信ユニットＴＶ９は、デジタルインターフェースＤ－Ｉ／Ｆ１０、復号化手段１１、認証要求手段１２、受信側認証手段１３、受信側複数認証ルール格納手段１４、受信側認証選択手段１５を持つ。この認証要求手段１２は、デジタルＡＶデータ送信ユニットＳＴＢ１に認証要求を出す手段である。また、受信側複数認証ルール格納手段１４は、送信側複数認証ルール格納手段５に格納された複数の認証ルールと同じ複数の種類の認証ルールを持つ手段である。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールを持つ。受信側認証選択手段１５は上述した受信側複数認証ルール格納手段１４から、送信側認証選択手段６で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段１３は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ１と認証を互いに交わす手段である。復号化手段１１はデジタルＡＶデータ送信ユニットＳＴＢ１で暗号化され送信されてきたデジタルＡＶデータをワーク鍵Ｋｗ１７を用いて復号

化する手段である。ワーク鍵Ｋｗ１７は前記受信側認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋｗ１６を生成する方法とともに後述する。デジタルインターフェースＤ－Ｉ／Ｆ１０は、送信ユニットＳＴＢ１とＡＶデータや信号のやりとりを行う手段である。

【００３２】

次に、このような本実施の形態の動作を説明する。

【００３３】

まず、デジタルＡＶデータ受信ユニットＴＶ９を構成する、認証要求手段１２が、デジタルインターフェースＤ－Ｉ／Ｆ１０を介して、デジタルＡＶデータ送信ユニットＳＴＢ１に自らのＩＤを含めて認証要求を出す。もちろんＡＶデータの送信要求も出す。デジタルＡＶデータ送信ユニットＳＴＢ１は、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ１は、まずデータ重要性判定手段３で、これから送信すべきＡＶデータ２の重要性を判定し場合分けする。すなわちＣＧＭＳの値が１１なら重要度は高く、そのデータは表示のみ可能であり、コピーすることは禁止される。また、ＣＧＭＳの値が１０の場合は一回のみコピー可能であり、比較的重要なデータである。またＣＧＭＳが００の場合は自由に視聴ないしはコピーして使用してよいので、重要でないデータと言える。またＣＧＭＳが０１となるＡＶデータは存在しない。このＣＧＭＳの値によりデータの重要度の場合分けがなされる。この結果は送信側認証選択手段６に送られ、送信側複数認証ルール格納手段５から最適な認証ルールが選択される。すなわち、最新の映画など重要なデータの場合には、時間がかかるが、偽造や改竄に強い、公開鍵と秘密鍵を用いる認証ルールが選択される。また、ニュースのような重要でないデータの場合には、時間はかからないが、偽造や改竄に弱い、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段７に送られ、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶ受信ユニットＴＶ９に送られる。デジタルＡＶ受信ユニットＴＶ９においては、受信側認証選択手段１５が、その選択情報を利用して受信側複数認証ルール格納手段１４から、デジタルＡＶデータ送信ユニットＳＴＢ１で選択された認証ルールと同じ認証ルールを選択す

る。従って選択されている認証ルールは送信側と受信側とで同じになる。そこで、受信側認証手段１３と送信側認証手段７とは互いに、デジタルインタフェースＤ－Ｉ／Ｆ１０およびデジタルインタフェースＤ－Ｉ／Ｆ８を介して、認証を行う。認証が成功すれば、後述するようにして送信側にワーク鍵Ｋｗ１６、また受信側にワーク鍵Ｋｗ１７が生成される。送信すべきデータ２は生成されたワーク鍵Ｋｗ１６を用いて、暗号化手段４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ８を介して、デジタルＡＶデータ受信ユニットＴＶ９に暗号化データとして送信される。デジタルインターフェースＤ－Ｉ／Ｆ１０を介して暗号化されたデータは、ワーク鍵Ｋｗ１７を用いて、復号化手段１１にて復号化され、データ１０１になる。これはデータ２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ１から、デジタルＡＶデータ受信ユニットＴＶ９にデータが送信されたことになる。

【００３４】

最後に、デジタルＡＶデータ受信ユニットＴＶ９は、ディスプレイ装置の画面にそのデータを表示する。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証手段が用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【００３５】

次に前述したようにデジタルＡＶデータ受信ユニットＴＶ９からデジタル送信ユニットＳＴＢ１に認証要求が出たときの認証のやりとりを示し、その結果ワーク鍵Ｋｗを生成する実施の形態を図４と図５を参照して説明する。

【００３６】

まず、図４に示すごとき、公開鍵と秘密鍵による認証を行う場合である。この場合受信側は秘密鍵Ｓｂと公開鍵Ｐｂを持つ。また送信側は秘密鍵Ｓａと公開鍵Ｐａを持つ。まずステップ１で受信側が乱数Ｂを発生する。受信側は自己の認識番号であるＩＤｂと乱数Ｂを自らの秘密鍵Ｓｂで暗号化した暗号文Ｓｂ（Ｂ）を送信側に送る。送信側は受信側の認識番号ＩＤｂから検索して受信側の公開鍵Ｐｂを入手する。ステップ８で入手した公開鍵Ｐｂで暗号文Ｓｂ（Ｂ）を復号化する。その結果ステップ９のごとく乱数Ｂが得られる。さらに、送信側は、ステッ

プ１０のごとく乱数Ａを発生する。乱数ＡとＢは送信側の秘密鍵Ｓａで暗号化され暗号文Ｓａ（Ａ，Ｂ）が作成される。送信側は暗号文Ｓａ（Ａ，Ｂ）と自己の認識番号ＩＤａを受信側に送信する。受信側は暗号文Ｓａ（Ａ，Ｂ）と送信側の認識番号ＩＤａを受け取る。受信側は、送信側の認識番号ＩＤａから検索して送信側の公開鍵Ｐａを入手し、ステップ２のごとく、Ｐａで暗号文Ｓａ（Ａ，Ｂ）を復号化する。ここで、暗号文Ｓａ（Ａ，Ｂ）から受信側にはステップ１で送った乱数Ｂと全く同一の乱数Ｂが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Ｐａ，Ｐｂは正当な者にしか入手できないようになっているものとする。次に受信側はステップ３のごとく、受信側の秘密鍵Ｓｂで乱数Ａを暗号化し、暗号文Ｓｂ（Ａ）を作成する。Ｓｂ（Ａ）は送信側に送られ、ステップ１１のごとく既に送信側で持っている、受信側の公開鍵Ｐｂで暗号文ＳＢ（Ａ）を復号化する。ステップ１０で発生した、乱数Ｂとステップ１１で復号化した乱数Ｂは全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記２つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【００３７】

今、受信側と送信側でやりとりした乱数ＡとＢは偽造や改竄が行われていないとすると、受信側と送信側以外の第３者には乱数ＡとＢは秘密の乱数である。そこで送信側で、ステップ１２のごとく、乱数ＡとＢを用いて鍵Ｋａｂを作成する。同じくステップ４のごとく受信側で乱数ＡとＢを用いて鍵Ｋａｂを作成する。前記２つのＫａｂは全く同一のものであり共通鍵となっている。次に送信側でステップ１３のごとく鍵Ｋｃを作成する。これを共通鍵Ｋａｂで暗号化し、暗号文Ｋａｂ（Ｋｃ）を作成して、受信側に送る。受信側はステップ５のごとく共通鍵Ｋａｂで暗号文Ｋａｂ（Ｋｃ）を復号化してＫｃを得、その結果、受信側が得た鍵Ｋｃと送信側にある鍵Ｋｃは全く同一であり、共通鍵となる。次に送信側でステップ１４のごとく鍵Ｋｗを作成する。鍵Ｋｗは共通鍵Ｋｃで暗号化され、暗号文Ｋｃ（Ｋｗ）として、受信側に送られる。受信側では、ステップ６のごとく共通鍵Ｋｃで暗号文Ｋｃ（Ｋｗ）を復号化し、ステップ７のごとくＫｗを得る。送

信側にある鍵Ｋｗと受信側にあるＫｗは全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵Ｋｗである。

次に図５に示すごとき、共通鍵による認証を行う場合の説明をする。この場合、送信側と受信側は共通鍵Ｓを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず,受信側でステップ１５のごとく２個の乱数Ａ１，Ａ２を発生し、共通鍵Ｓで暗号化し、暗号文Ｓ（Ａ１Ａ２）を作成し、送信側へ送る。送信側ではステップ２０のごとく共通鍵Ｓで暗号文Ｓ（Ａ１Ａ２）を復合化する。そうすると、ステップ２１のごとく乱数Ａ１と乱数Ａ２が得られる。送信側は乱数Ａ２を受信側に送る。受信側はステップ１６のごとく２つの乱数Ａ１とＡ２を持つことになる。ステップ１５で発生した乱数Ａ２とステップ１６で送信側から受け取った乱数Ａ２が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記２つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ２２のごとく乱数Ｂ１とＢ２を発生し、暗号化して、暗号文Ｓ（Ｂ１Ｂ２）を受信側に送る。受信側はステップ１７のごとく共通鍵Ｓを用いて暗号文Ｓ（Ｂ１Ｂ２）を復号化する。すると、ステップ１８のごとく乱数Ｂ１とＢ２が得られる。受信側は乱数Ｂ２を送信側に送る。送信側はステップ２３のごとく乱数Ｂ１とＢ２を持つことになる。ステップ２２で発生した乱数と、ステップ２３で受信側から受け取った乱数Ｂ２が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記２つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【００３８】

ここまでで、認証が成功しているとすると、乱数Ａ１と乱数Ｂ１は送信側と受信側以外の第３者には秘密の乱数である。送信側ではステップ２４のごとく乱数Ａ１と乱数Ｂ1から鍵Ｋｗを作成する。一方受信側では、ステップ１９のごとく乱数Ａ１と乱数Ｂ１から鍵Ｋｗを作成する。送信側にある鍵Ｋｗと受信側にある鍵Ｋｗは全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵Ｋｗである。

【００３９】

なお、本発明において、選択する認証ルールの種類は、前記公開鍵及び秘密鍵と共通鍵との２種類に限らず、その他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００４０】

なお、本実施の形態の変形例として、デジタルＡＶデータ送信ユニット１はデジタルAV受信ユニット９と同じ機能を有し、また、デジタルＡＶデータ受信ユニット９はデジタルＡＶ送信ユニット１と同じ機能を有するようになっていてもよい。以後それらのユニットのことを、デジタルＡＶデータ送受信ユニットと呼ぶ。またそれらの送受信ユニットが３台以上が互いに接続されていてもよい。

【００４１】

次に本発明の第二の実施の形態について図６を参照して説明する。

【００４２】

本実施の形態では、第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対して、デジタルＡＶデータ受信ユニットＶＴＲ４５が有する認証ルールの種類によって、認証ルールを選択するところが、相違点である。

【００４３】

デジタルＡＶデータ送信ユニットＳＴＢ３８は、送信側複数認証ルール格納手段４１等を持つ。送信側複数認証ルール格納手段４１は、複数種類の認証ルールを持つ手段である。これは第一の実施の形態で説明したごとく、例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。ユニット認証ルール情報受信手段４２は、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られて来た認証ルールに関連する情報を受信する手段である。送信側認証取り出し手段５３は、その認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段４１から所定の認証ルールを取り出し、送信側認証手段４３に渡す手段である。送信側認証手段４３は、デジタルＡＶ受信ユニットＶＴＲ４５と互いに認証を交わす手段である。暗号化手段４０は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋｗ５３により、データ３９を暗号化する手段である。デジタルインター

フェースＤ－Ｕ／Ｆ４４は、デジタルＡＶデータ受信ユニットＶＴＲ４５とデータや信号のやりとりをする手段である。

【００４４】

デジタルＡＶデータ受信ユニットＶＴＲ４５は、受信側認証ルール格納手段４９等を持つ。この受信側認証ルール格納手段４９は、第一の実施の形態で説明した場合とは違って、一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段４９に格納されている認証ルールはデジタルＡＶデータ受信ユニットＶＴＲ４５の装置の性質あるいは重要度によって、あらかじめ決められている。すなわちデータの再利用を予定しないＴＶなどのユニットには時間はかかるが、偽造や改竄に強い認証ルールが格納されており、またデータのコピーを前提とするＶＴＲのようなユニットには、時間はかからないが、偽造や改竄に弱い認証ルールが格納されている。これによって、ＡＶデータの著作権を守ることができる。本実施の形態では　デジタルＡＶデータ受信ユニットＶＴＲ４５はＶＴＲであるので、受信側認証ルール格納手段４９は共通鍵を持つものとして説明をする。認証ルール情報送信手段５０は、デジタルＡＶデータ受信ユニットＶＴＲ４５が受信側認証ルール格納手段４９に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段５１は、デジタルＡＶ送信ユニットＳＴＢ３８と互いに認証を交わす手段である。復号化手段４７は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋｗ５４により、暗号化されたデータを復号化する手段である。

【００４５】

次にこのような本実施の形態の動作を説明する。

【００４６】

まず、デジタルＡＶデータ受信ユニットＶＴＲ４５を構成する、認証要求手段４８がデジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ３８は、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、前記認証要求

を受信する。また同時に、認証ルール情報送信手段５０が、受信側認証ルール格納手段４９を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４６を介して、デジタルＡＶデータ送信ユニットＳＴＢ３８に送る。ユニット認証ルール情報受信手段４２が、デジタルＡＶデータ受信ユニットＶＴＲ４５から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ４４を介して、受け取る。さらに、この認証ルールの識別子は、送信側認証取り出し手段５３に渡され、送信側複数認証ルール格納手段４１から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出す。その後、取り出された共通鍵による認証ルールは、送信側認証手段４３に渡される。その後、送信側認証手段４３と受信側認証手段５１は互いに、デジタルインターフェースＤ－Ｉ／Ｆ４４とＤ－Ｉ／Ｆ４６を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で説明したごとく、送信側にワーク鍵Ｋｗ５３、受信側にワーク鍵Ｋｗ５４が生成される。データ３９は暗号化手段４０にてワーク鍵Ｋｗ５３により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ４４を介して、デジタルＡＶ受信ユニットＶＴＲ４５に送られる。デジタルインターフェースＤ－Ｉ／Ｆ４６を介して暗号化されたデータは、復号化手段４７に送られ、ワーク鍵Ｋｗ５４を用いて復号化され、データ５２が得られる。

【００４７】

なお、本発明において、送信側の認証ルールの種類は、前記共通鍵に限らず、公開鍵及び秘密鍵、またその他の種類でもよく、更に３種類以上の異なる認証ルールを使用するものであってもよい。

【００４８】

なお、デジタルＡＶデータ受信ユニットは２台あり、その一つは共通鍵による認証ルールのみ有し、他の一つは公開鍵及び秘密鍵のみを有するものであってもよい。さらに３台以上のデジタルＡＶデータ受信ユニットであってもよい。

【００４９】

次に本発明の第三の実施の形態について図７を参照して説明する。

【００５０】

第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対し、また、第二の実施の形態がデジタルＡＶデータ受信ユニットの種類によって認証ルールを変えていたのに対し、本実施の形態では、データの重要度とデジタルＡＶ受信ユニットの種類の両方で認証ルールを決めるところが特徴である。

【００５１】

本実施の形態では、デジタルＡＶデータ送信ユニットＳＴＢ５６と、複数認証デジタルＡＶデータ受信ユニットＴＶ６５と、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の三種類のユニットを扱う。デジタルＡＶデータ送信ユニットＳＴＢ５６は複数認証デジタルＡＶデータ受信ユニットＴＶ６５と単一認証デジタルAVデータ受信ユニットＶＴＲ７２にデータを送信するユニットである。複数認証デジタルＡＶデータ受信ユニットＴＶ６５に対しては、デジタルＡＶデータ送信ユニットＳＴＢ５６においてデータの重要度により複数種類の認証ルールを選択して、そのデータを送信する。また、単一デジタルＡＶデータ受信ユニットVTR72は自らの持つ一つの認証ルールを用いてデジタルAVデータ送信ユニットＳＴＢ５６とで認証を行うユニットである。

【００５２】

デジタルＡＶデータ送信ユニットＳＴＢ５６は、データ重要性判定手段５７を持つ。これは、データ８２の重要性を重要度に応じて複数種類の場合分けを行う手段である。この重要度は第一の実施の形態で説明したごとくＣＧＭＳで表現されている。このＣＧＭＳは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段６４は、データ８２を認証の過程で作成されたワーク鍵Ｋｗ６４で暗号化する手段である。ワーク鍵Ｋｗ１６を生成する過程は第一の実施の形態で説明した。送信側複数認証ルール格納手段６３は、複数種類の認証ルールを持つ。例えば、公開鍵と秘密鍵を用いた認証ルールや、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段５９は、送信側複数認証ルール格納手段６３が持つ複数種類の認証ルールから

一種類の認証ルールを選択する手段である。この時、データ重要性判定手段５７の場合分けの結果を参考にする。第一の実施の形態のごとく、本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱い、共通鍵を用いた認証ルールを選択する。ユニット認証ルール情報受信手段６０は、デジタルＡＶデータ受信ユニットＴＶ７２から送られて来た認証ルールに関する情報を受信する手段である。送信側認証ルール取り出し手段５８は、認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段６３から所定の認証ルールを取り出し、送信側認証手段６１に渡す手段である。送信側認証手段６１は、実際に複数認証デジタルＡＶデータ受信ユニットＴＶ６５及び単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２と認証を交わす手段である。デジタルインターフェースＤ－Ｉ／Ｆ６２は、複数認証デジタルＡＶデータ受信ユニットＴＶ６５や単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２とＡＶデータや信号をやりとりする手段である。

【００５３】

複数認証デジタルＡＶデータ受信ユニットＴＶ６５は、認証要求手段６７を持つ。これは、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す手段である。また、受信側複数認証ルール格納手段６８は、送信側複数認証ルール格納手段６３と同じ複数種類の認証ルールを持つ。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールがある。受信側認証選択手段６９は、受信側複数認証ルール格納手段６８から、送信側認証選択手段５９で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段７０は、その選択された認証ルールで、つまりデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールを用いて実際にデジタルＡＶデータ送信ユニットＳＴＢ５６と認証を互いに交わす手段である。復号化手段６６は、デジタルＡＶデータ送信ユニットＳＴＢ５６で暗号化されたデジタルＡＶデータをワーク鍵Ｋｗ８０を用いて復号化する手段である。ワーク鍵Ｋｗ８０は前記認証過程で生成されるもので、その生成する方法は前記ワーク鍵Ｋｗ７９とともに第一の実施の形態で説明した。デジタルインターフェースＤ－Ｉ／Ｆ７１は、

デジタルＡＶデータ送信ユニットＳＴＢ５６とＡＶデータや信号のやりとりを行う手段である。

【００５４】

単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２は、受信側認証ルール格納手段７５を持つ。これは、前述したごとく一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段７５に格納されている認証ルールは単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２の装置の種類や、重要度によって、あらかじめ決められている。ここでは、受信側認証ルール格納手段７５が共通鍵を持つものとして説明をする。認証ルール情報送信手段７６は、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２が受信側認証ルール格納手段７５に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段７７は、デジタルＡＶデータ送信ユニットと互いに認証を交わす手段である。復号化手段７３は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Ｋｗ８１により、暗号化されたデータを復号化する手段である。

【００５５】

次にこのような本実施の形態の動作を説明する。

【００５６】

まず、はじめに複数認証デジタルＡＶデータ受信ユニットＴＶ６５かまたは単一認証デジタルＡＶデータ受信ユニット７２が認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６はどのユニットから認証要求が送られて来たのかを判断する。

【００５７】

以下、まず複数認証デジタルＡＶデータ受信ユニットＴＶ６５から認証要求が来た場合を説明し、次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の説明を行う。

【００５８】

第一に、前述したように複数認証デジタルＡＶデータ受信ユニットＴＶ６５を

構成する、認証要求手段６７が、デジタルインターフェースＤ－Ｉ／Ｆ７１を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に自らのＩＤを含めて認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。そうするとデジタルＡＶデータ送信ユニットＳＴＢ５６は、まずデータ重要性判定手段５７で、これから送信すべきデータ８２の重要性を判定し場合分けする。この結果は送信側認証選択手段５９に送られ、送信側複数認証ルール格納手段６３から最適な認証ルールが選択される。すなわち、重要なデータの場合には、公開鍵と秘密鍵を用いる認証ルールが選択される。また、重要でないデータの場合には、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段６１に送られ、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットに送られる。複数認証デジタルＡＶデータ受信ユニットにおいては、受信側認証選択手段６９が、その選択情報を利用して受信側複数認証ルール格納手段６８からデジタルＡＶデータ送信ユニットＳＴＢ５６で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。受信側認証手段７０と送信側認証手段６１とは互いに、デジタルインターフェースＤ－Ｉ／Ｆ７１およびデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、認証を行う。認証が成功すれば、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋｗ７９、また受信側にワーク鍵Ｋｗ８０が生成される。送信すべきデータ８２は生成されたワーク鍵Ｋｗ７９を用いて、暗号化手段６４で暗号化される。そのあと、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、複数認証デジタルＡＶデータ受信ユニットＴＶ６５に暗号化されたデータとして送信される。デジタルインターフェースＤ－Ｉ／Ｆ７１を介して暗号化されたデータは、ワーク鍵Ｋｗ８０を用いて、復号化手段６６にて復号化され、データ８３になる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、複数認証デジタルＡＶデータ受信ユニットＴＶ６５にデータが送信されたことになる。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証ルールが用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが

用いられる。

【００５９】

次に単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から認証要求が来た場合の動作の説明を行う。まず、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２を構成する、認証要求手段７４がデジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に認証要求を出す。デジタルＡＶデータ送信ユニットＳＴＢ５６は、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、前記認証要求を受信する。同時に認証ルール情報送信手段７６が、受信側認証ルール格納手段７５を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースＤ－Ｉ／Ｆ７８を介して、デジタルＡＶデータ送信ユニットＳＴＢ５６に送る。ユニット認証ルール情報受信手段６０が、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースＤ－Ｉ／Ｆ６２を介して、受け取る。さらにこの認証ルールの識別子は、送信側認証ルール取り出し手段５８に渡され、送信側複数認証ルール格納手段６３から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールは、送信側認証手段６１に渡される。送信側認証手段６１と受信側認証手段７７は互いに、デジタルインターフェースＤ－Ｉ／Ｆ６２とＤ－Ｉ／Ｆ７８を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で詳述したごとく、送信側にワーク鍵Ｋｗ７９、受信側にワーク鍵Ｋｗ８１が生成される。認証の結果ワーク鍵が生成される過程は、第一の実施の形態で詳述した。データ８２は暗号化手段６４にてワーク鍵Ｋｗ７９により暗号化される。暗号化されたデータはデジタルインターフェースＤ－Ｉ／Ｆ６２を介して、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２に送られる。デジタルインターフェースＤ－Ｉ／Ｆ７８を介して暗号化されたデータは、復号化手段Ｋｗ８１に送られ、ワーク鍵Ｋｗ８１を用いて復号化され、データ８４が得られる。これはデータ８２と同一のデータであり、デジタルＡＶデータ送信ユニットＳＴＢ５６から、単一認証デジタルＡＶデータ受信ユニットＶＴＲ７２に

データが送信されたことになる。

【００６０】

次に、本発明の第四の実施の形態を説明する。

【００６１】

本実施の形態では、デジタルAVデータ受信ユニットが正当なものか不正なものかを調べて作成しておいた管理基準（ＣＲＬ）を利用するものである。そのＣＲＬの作成の仕方は、例えば、消費者が購入した販売店が発行した登録カードを元に作成する方法等が考えれれる。

【００６２】

図８は、その管理基準を放送局から送られてくるデジタルAVデータの重要度に応じて、その管理基準を参照するかどうか決定するものである。

【００６３】

デジタルＡＶ送信ユニットＳＴＢ９３は、放送局から送られてくるデジタルＡＶデータの重要度に応じて、データの重要性を判定する、データ重要性判定手段８６を有する。また、データの重要度に応じて管理基準格納手段８８に格納されている管理基準情報（ＣＲＬ）を参照するかどうかを判定する、管理基準参照決定手段８７を有する。また、前記決定結果に従って、認証を行うかどうかを決定する、認証決定手段８９を有する。また、実際にデジタルＡＶデータ受信ユニットＴＶ９２と認証を交わす、認証手段９０を有する。前記認証手段９０は、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶデータ受信ユニットＴＶ９２に接続している。

【００６４】

次に本実施の形態の動作を説明する。まず、放送局から送られてくるデジタルＡＶデータ８５は、データ重要性判定手段８６で、重要性を判定される。その結果は、管理基準参照決定手段８７に渡され、管理基準格納手段８８に格納されている情報を参照すべきかどうか決定される。例えば、新作の映画等の場合は重要なので、管理基準情報を参照すると決定する。また、ニュース等の場合は重要でないので、管理基準情報を参照しないと決定する。さらに認証決定手段８９で、前記管理基準参照決定手段８７の判定決定に従って、認証すべきかどうか決定さ

れる。すなわち、デジタルAVデータ受信ユニットＴＶ９２が、デジタルＡＶデータ８５を受信するのに正当な機器か不当な機器かを、管理基準格納手段８８に格納されている管理基準情報で判断される。正当であると判断されれば、次の認証手段９０で、デジタルインターフェースＤ－Ｉ／Ｆ９１を介して、デジタルＡＶ受信ユニットＴＶ９２と認証が交わされる。不当と判断されればその時点で、デジタルＡＶデータ受信ユニットとの認証は交わされず、データ８５の送信はされない。

【００６５】

他方、図９は上述した管理基準を、デジタルＡＶデータ受信ユニットの装置の種類、あるいは重要度に応じて、その管理基準を参照するかどうか決定するものである。

【００６６】

デジタルＡＶデータ送信ユニットＳＴＢ９４は、デジタルＡＶデータ受信ユニット１００の装置の種類あるいは、重要度に応じて、その管理基準格納手段９６を参照すべきかどうかを決定する、管理基準参照決定手段９５を有する。また、認証決定手段９７は、認証するかどうかを決定する。管理基準格納手段９６は、デジタルＡＶ受信ユニット１００がデジタルＡＶデータを受信するのに正当な機器か正当でない機器かの情報が格納されている。認証手段９８は、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、デジタルＡＶデータ受信ユニットＶＴＲ１００と認証を行う。

【００６７】

次に本実施の形態の動作を説明する。まず、デジタルＡＶデータ受信ユニットＶＴＲ１００が、デジタルインターフェースＤ－Ｉ／Ｆ９９を介して、管理基準参照決定手段９５に機器情報を送る。これを受けて、管理基準参照決定手段９５は、管理基準格納手段９６に格納されている情報を参照すべきかどうかを決定する。管理基準格納手段９６を参照すると決定された場合は、認証決定手段９７は、まず、管理基準格納手段９６を参照して、デジタルＡＶデータ受信ユニットがデータを受信するのに正当な機器か、不正な機器かを判定する。ここで、正当な機器と判定されれば、次の認証手段９８にて、デジタルインターフェースＤ－Ｉ

／Ｆ９９を介して、デジタルＡＶデータ受信ユニットと認証を開始する。デジタルＡＶデータ受信ユニットがデータを受信するのに不正な機器と判定された場合は、認証は行われず、データの送信も行われない。

【００６８】

なお、ＳＴＢを送信ユニットとして説明してきたが、ＶＴＲで録画したデータを再生する際には、前記ＶＴＲが送信ユニットとなる。この際ＣＧＭＳが入力時「１回コピー可」であれば「コピー不可」に書きかえられて出力される。ここで、データの重要度としては、元の入力時における重要度と考えるべきであり、「１回コピー可」と同様の認証ルールを使うこともできる。このように「１回コピーの結果コピー不可となったデータ」と「元からコピー不可のデータ」を見分ける必要がある際には、前述した、存在しないＣＧＭＳ値０１を前者の区別用に割り当てることもできる。

【００６９】

さらに、本発明の各構成要素は、それぞれの機能を実現する専用のハード回路、機器等で実現しても、あるいは、コンピュータを利用してソフトウェア的に実現してもかまわない。

【００７０】

さらに、本発明をコンピュータで実現する場合、それらの各構成要素の機能の全部又は一部を実現するためのプログラムを格納した媒体も本発明に属する。

【００７１】

【発明の効果】

以上説明したところから明らかなように、本発明は、重要でないデータの認証に多くの時間を要せず、重要なデータに関しては、その認証が偽造や改竄に強くまた、ユニットによって認証に必要な厳密さを変えることによって、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、システム等を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第一の実施の形態についての概略図

【図２】

従来技術について示す概略図

【図３】

従来技術について示す概略図

【図４】

本発明の実施の形態のうち認証方法に関するブロック図

【図５】

本発明の実施の形態のうち認証方法に関するブロック図

【図６】

本発明の第二の実施の形態についての概略図

【図７】

本発明の第三の実施の形態についての概略図

【図８】

本発明の第四の実施の形態についての概略図

【図９】

本発明の第四の実施の形態についての概略図

【符号の説明】

１　ＳＴＢ

３　データ重要性判定手段

５　送信側複数認証ルール格納手段

６　送信側認証選択手段

７　送信側認証手段

９　ＴＶ

１３　受信側認証手段

１４　受信側複数認証ルール格納手段

１５　受信側認証選択手段

１８　ＳＴＢ

１９　認証手段

２０　公開鍵／秘密鍵

２３　ＴＶ

２５　認証手段

２６　公開鍵／秘密鍵

２８　ＳＴＢ

２９　認証手段

３０　共通鍵

３３　ＴＶ

３５　認証手段

３６　共通鍵

３８　ＳＴＢ

４１　送信側複数認証ルール格納手段

４２　ユニット認証ルール情報受信手段

４３　送信側認証手段

４５　ＶＴＲ

４８　認証要求手段

４９　受信側認証ルール格納手段

５０　認証ルール情報送信手段

５１　受信側認証手段

５５　送信側認証ルール取り出し手段

５６　ＳＴＢ

５７　データ重要性判定手段

５８　送信側認証ルール取り出し手段

５９　送信側認証選択手段

６０　ユニット認証ルール情報受信手段

６１　送信側認証手段

６３　送信側複数認証ルール格納手段

６５　ＴＶ

６７　認証要求手段

６８　受信側複数認証ルール格納手段

６９　受信側認証選択手段

７０　受信側認証手段

７２　ＶＴＲ

７４　認証要求手段

７５　受信側認証ルール格納手段

７６　認証ルール情報送信手段

７７　受信側認証手段

８６　データ重要性判定手段

８７　管理基準参照決定手段

８８　管理基準格納手段

８９　認証決定手段

９０　認証手段

９２　ＴＶ

９３　ＳＴＢ

９４　ＳＴＢ

９５　管理基準参照決定手段

９６　管理基準格納手段

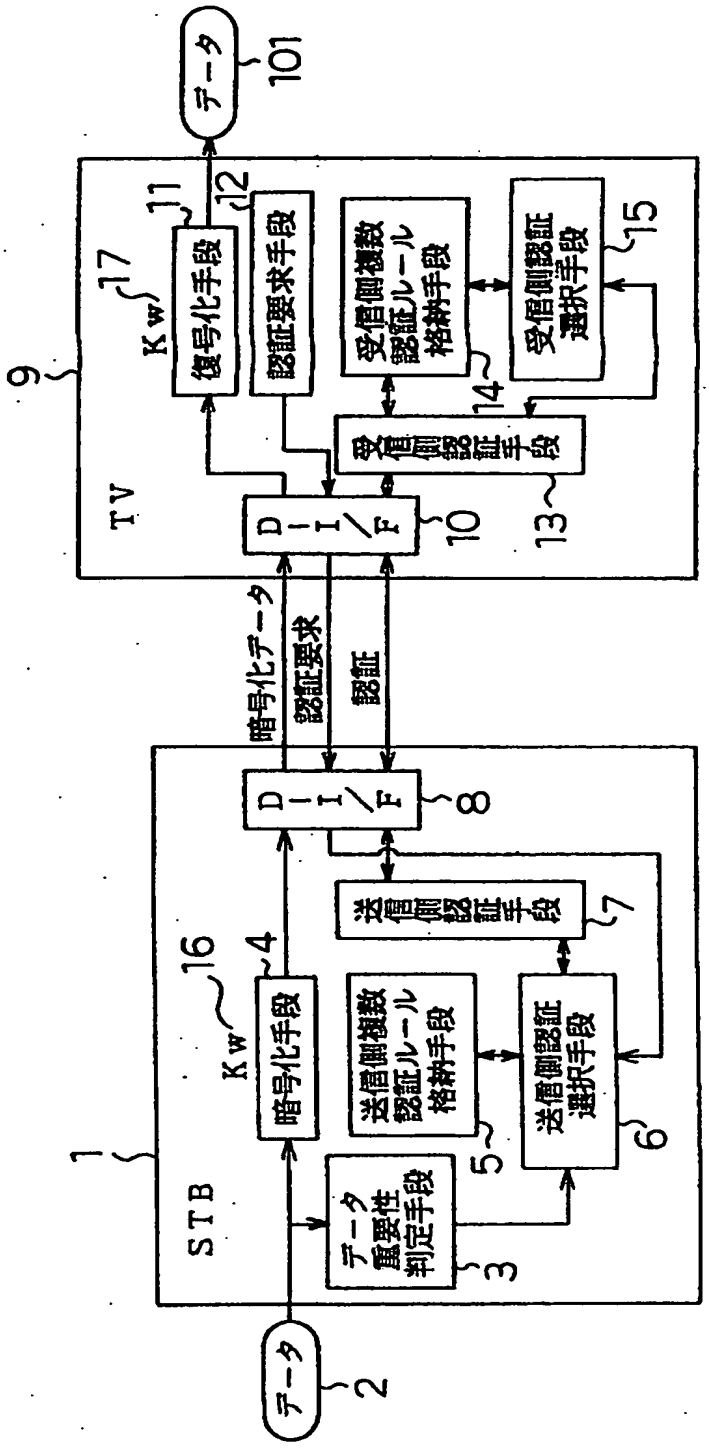
９７　認証決定手段

９８　認証手段

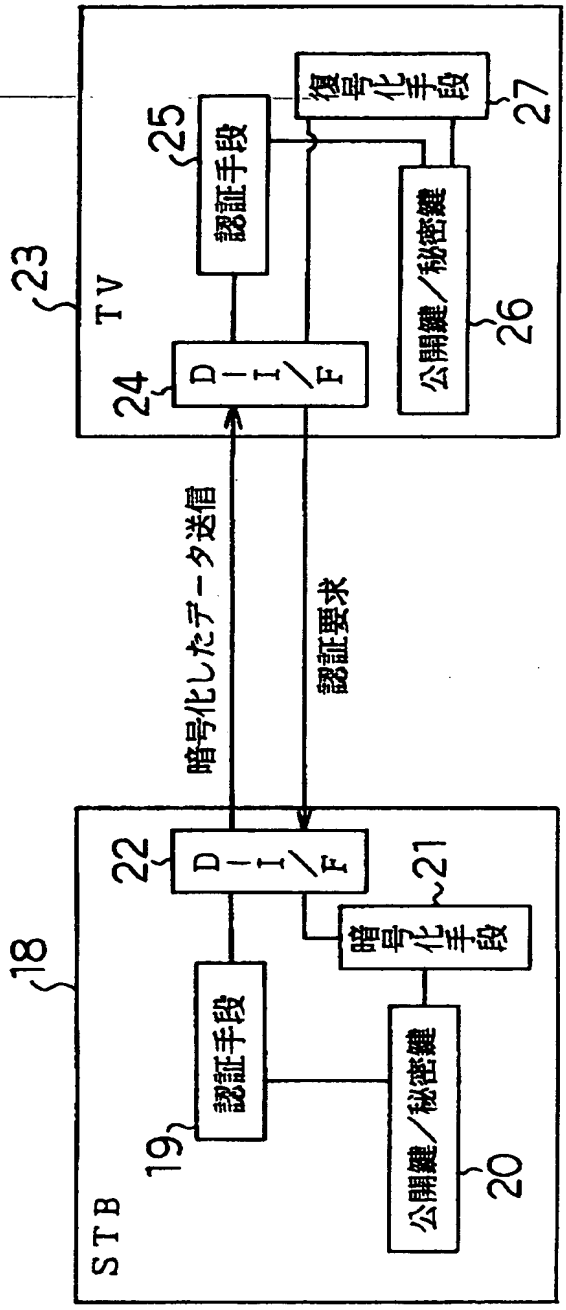
１００　ＶＴＲ

【書類名】　図面

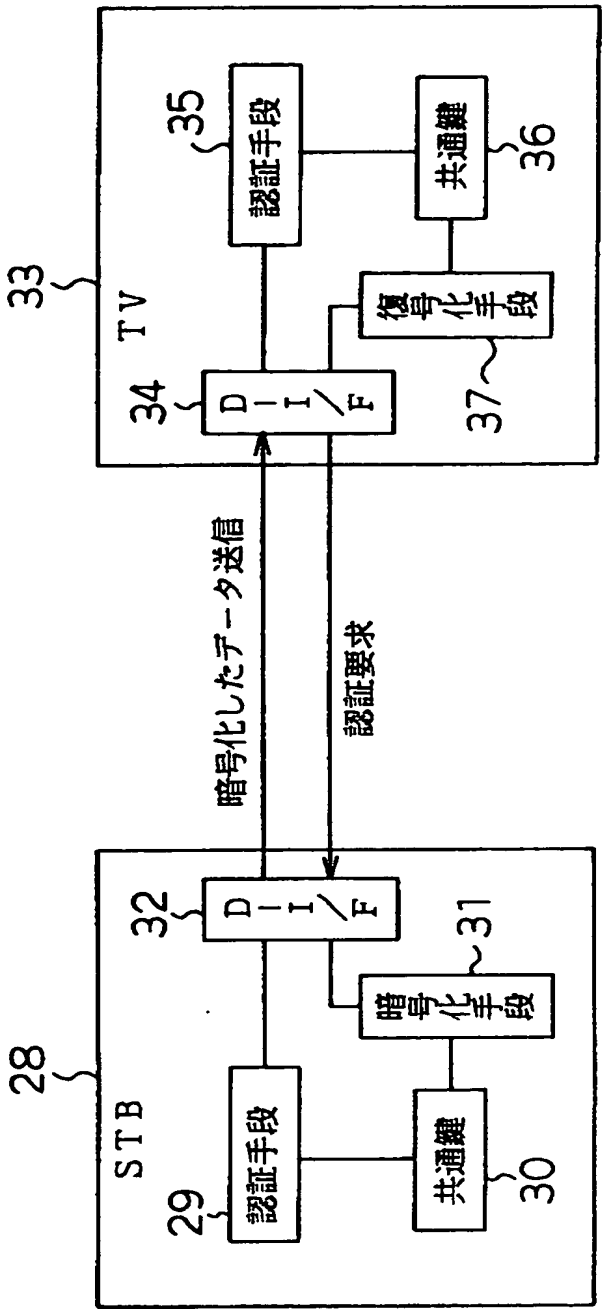
【図１】


データ
101
TV
9
Kw
17
復号化手段
11
認証要求手段
12
受信側複数認証ルール格納手段
14
受信側認証選択手段
15
受信側認証手段
13
D-I/F
10
暗号化データ
認証要求
認証
D-I/F
8
送信側認証手段
7
16
Kw
暗号化手段
4
送信側複数認証ルール格納手段
5
送信側認証選択手段
6
STB
1
データ重要性判定手段
3
データ
2

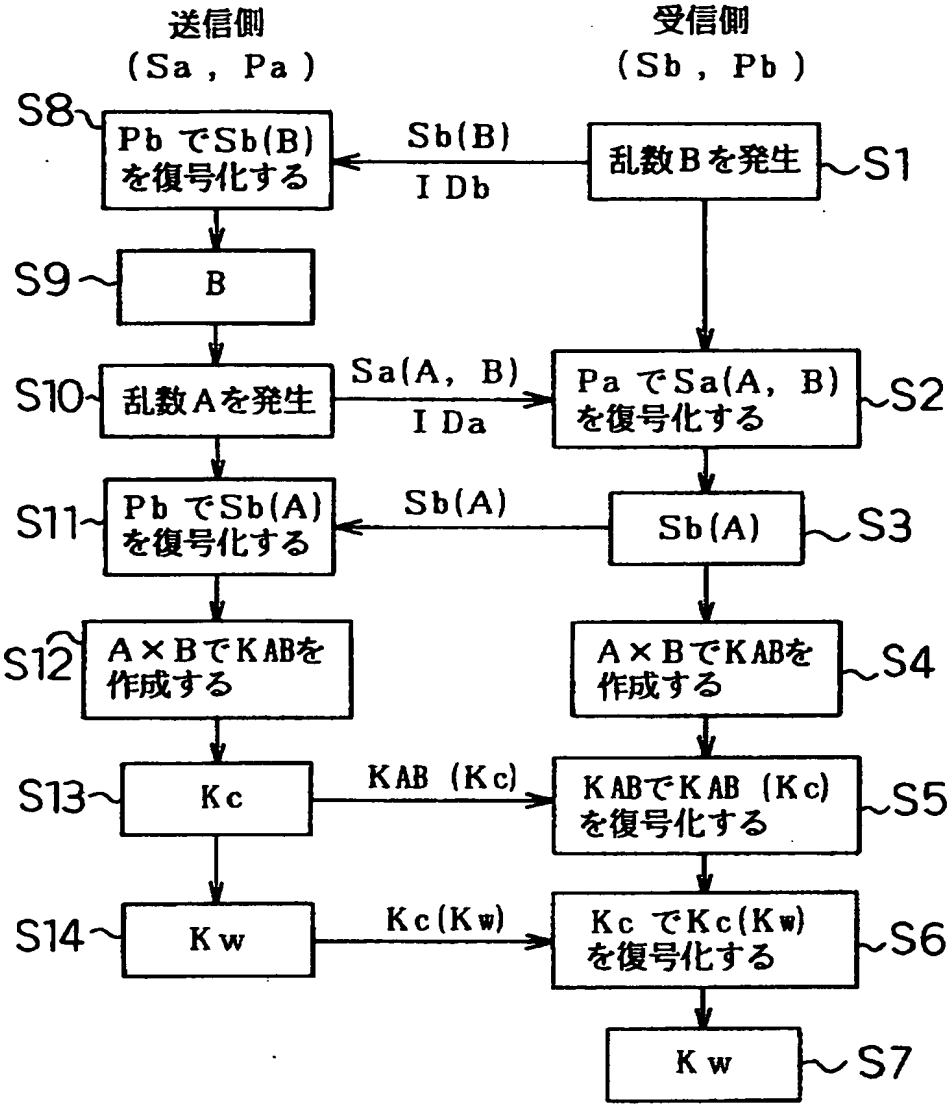
【図２】


TV
23
認証手段
25
復号化手段
27
D－I／F
24
公開鍵／秘密鍵
26
暗号化したデータ送信
認証要求
STB
18
D－I／F
22
暗号化手段
21
認証手段
19
公開鍵／秘密鍵
20

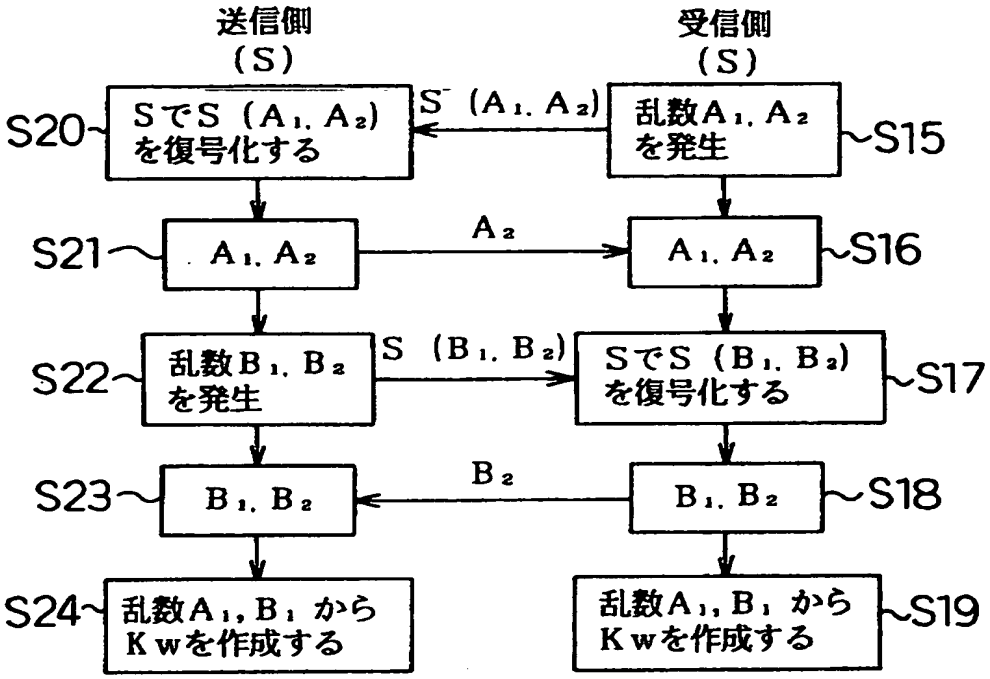
【図３】


33
TV
35
認証手段
共通鍵
36
復号化手段
37
34
D－I／F
暗号化したデータ送信
認証要求
32
D－I／F
31
暗号化手段
28
STB
29
認証手段
共通鍵
30

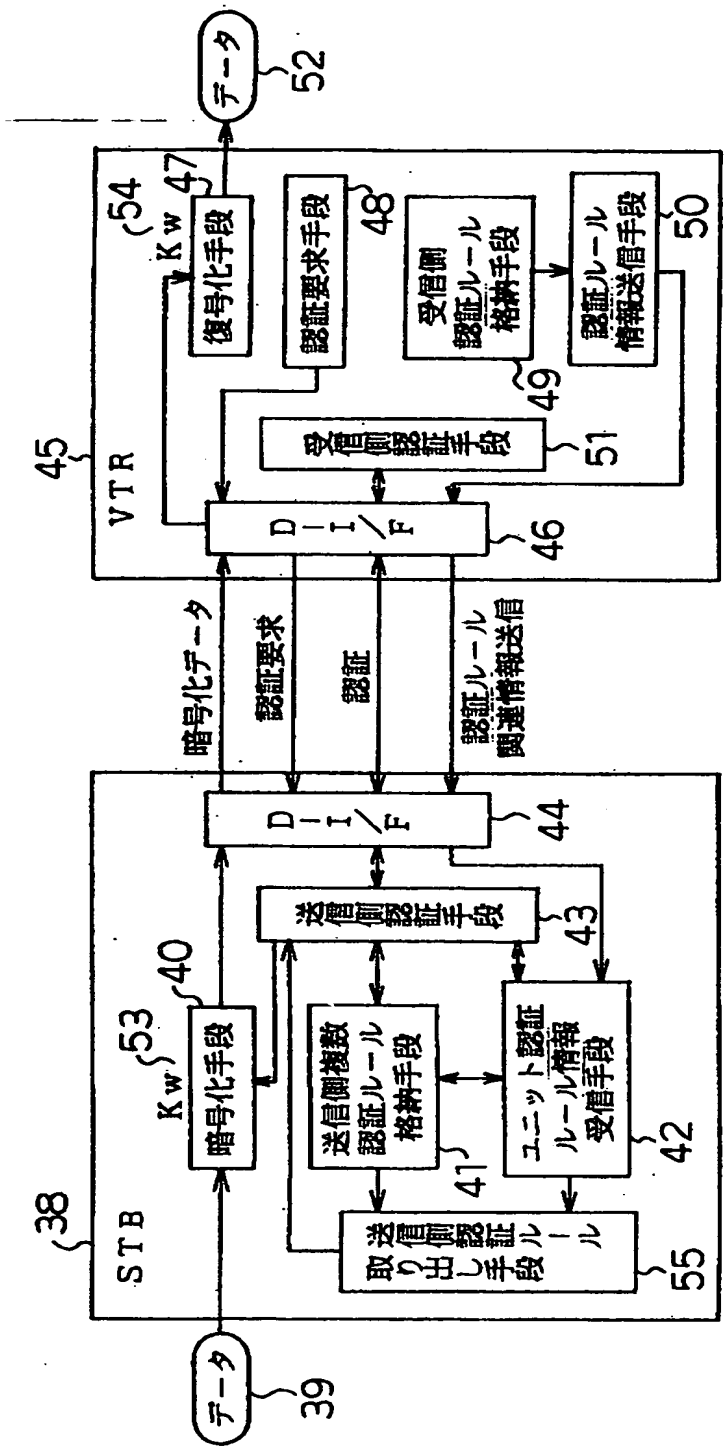
【図４】


送信側
(Sa , Pa)
受信側
(Sb , Pb)
S8
Pb でSb(B)
を復号化する
Sb(B)
I Db
乱数Bを発生
S1
S9
B
S10
乱数Aを発生
Sa(A, B)
I Da
Pa でSa(A, B)
を復号化する
S2
S11
Pb でSb(A)
を復号化する
Sb(A)
Sb(A)
S3
S12
A×BでKABを
作成する
A×BでKABを
作成する
S4
S13
Kc
KAB (Kc)
KABでKAB (Kc)
を復号化する
S5
S14
Kw
Kc(Kw)
Kc でKc(Kw)
を復号化する
S6
Kw
S7

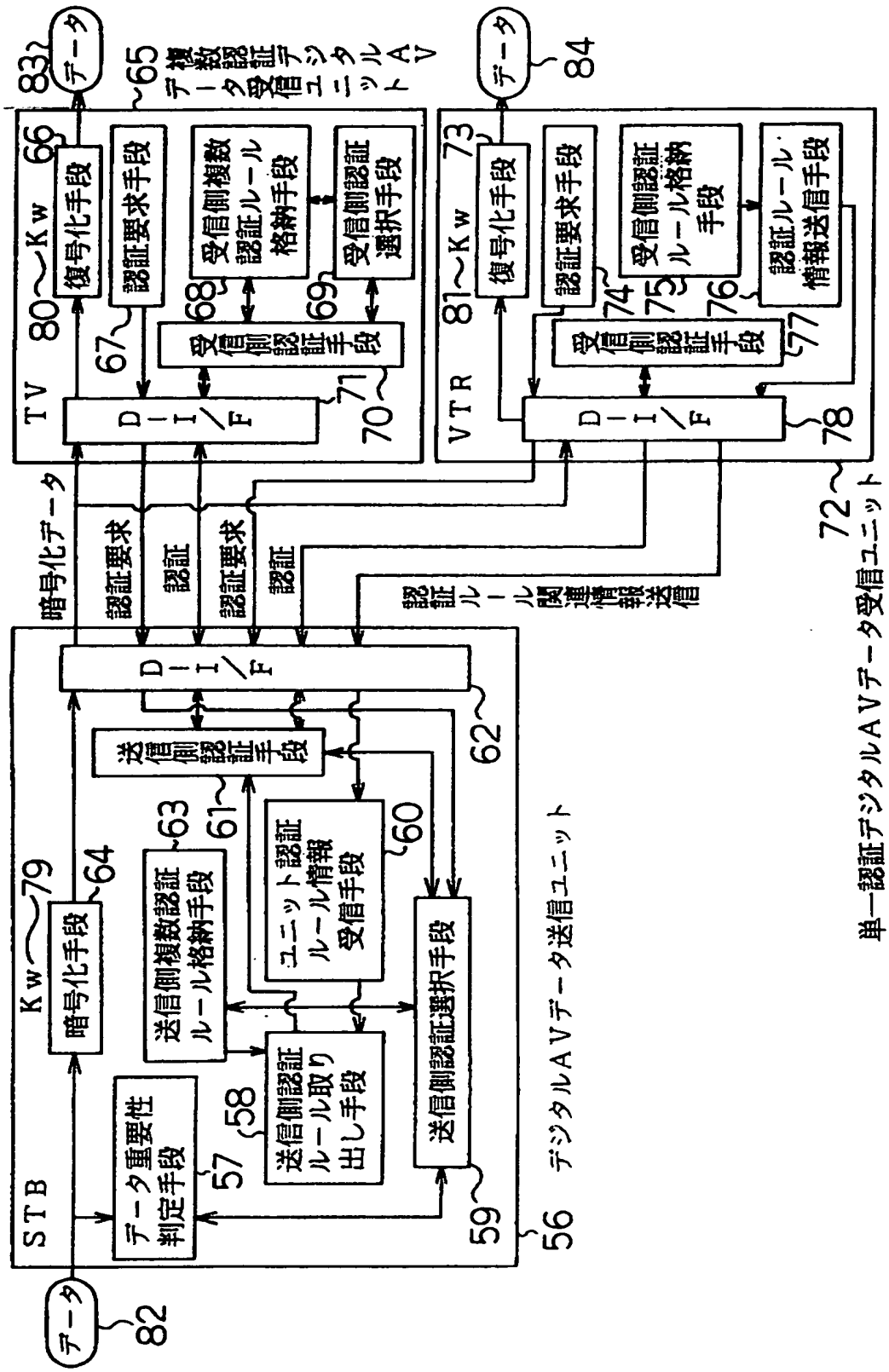
【図５】


送信側
(S)
受信側
(S)
S20
SでS (A1, A2)
を復号化する
S (A1, A2)
乱数A1, A2
を発生
S15
S21
A1, A2
A2
A1, A2
S16
S22
乱数B1, B2
を発生
S (B1, B2)
SでS (B1, B2)
を復号化する
S17
S23
B1, B2
B2
B1, B2
S18
S24
乱数A1, B1 から
Kwを作成する
乱数A1, B1 から
Kwを作成する
S19

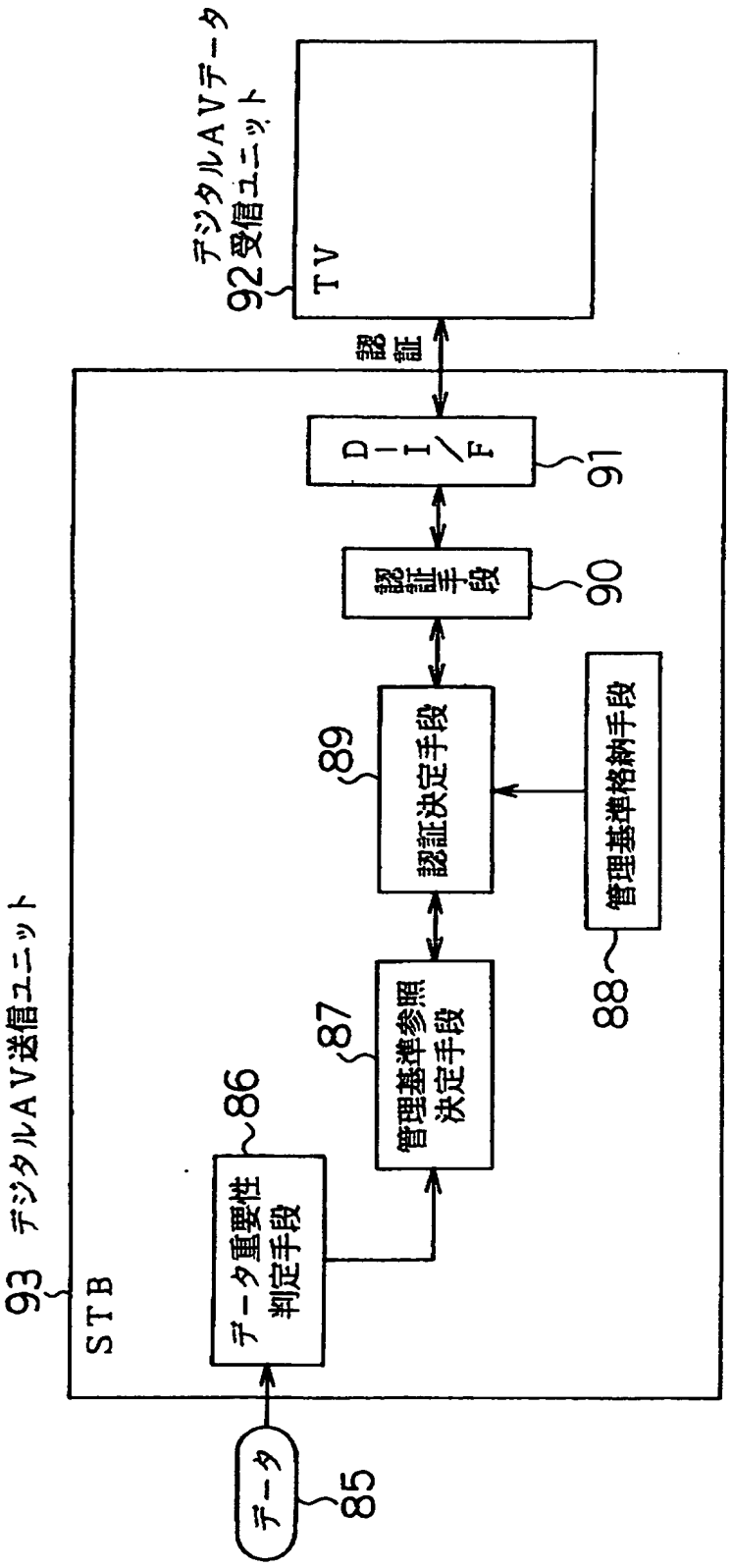
【図６】


データ
52
54
Kw
47
復号化手段
認証要求手段
48
受信側認証ルール格納手段
49
認証ルール情報送信手段
50
受信側認証手段
51
45
VTR
D－I／F
46
暗号化データ
認証要求
認証
認証ルール関連情報送信
D－I／F
44
送信側認証手段
43
40
53
Kw
暗号化手段
送信側複数認証ルール格納手段
41
ユニット認証ルール情報受信手段
42
38
STB
送信側認証ルール取り出し手段
55
データ
39

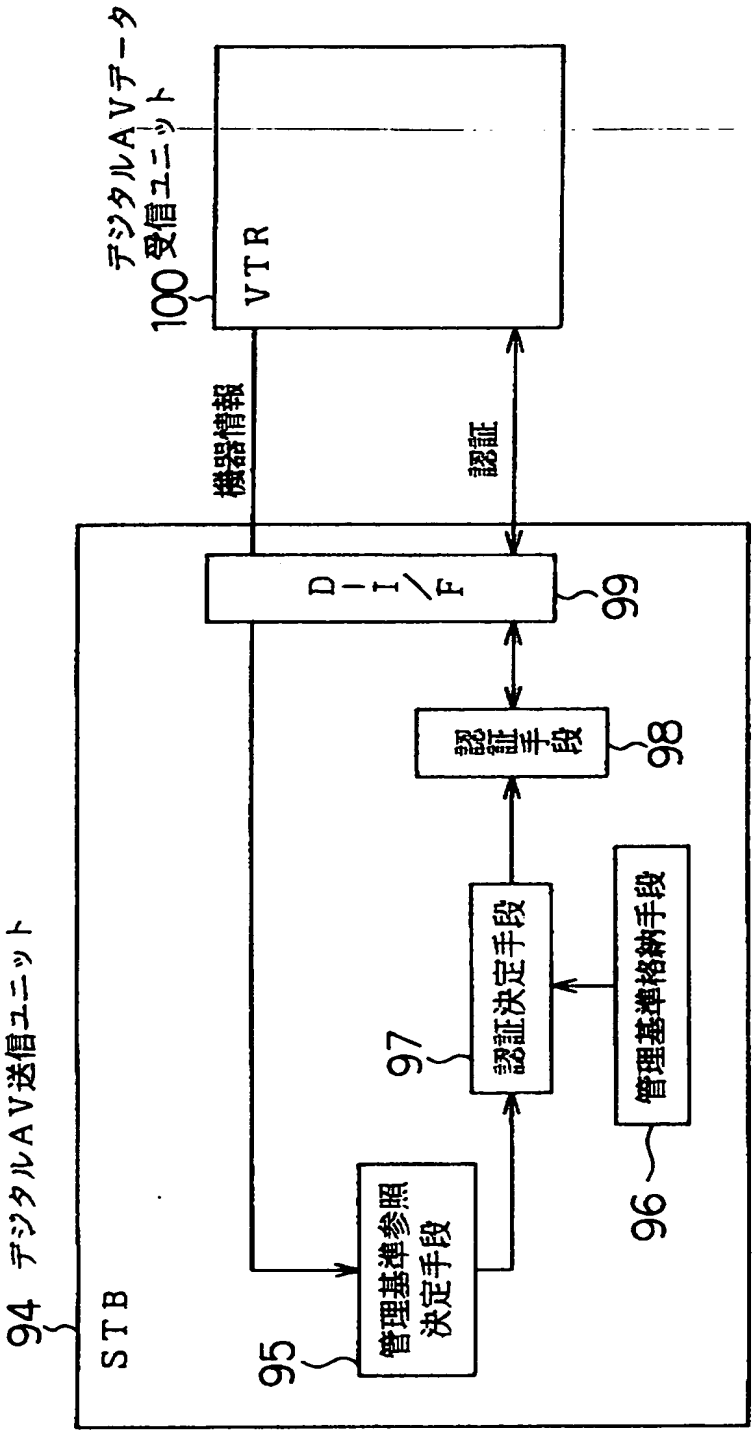
【図７】


TV
VTR
STB
D－I／F
復号化手段
認証要求手段
受信側複数認証ルール格納手段
受信側認証選択手段
受信側認証手段
暗号化手段
送信側複数認証ルール格納手段
ユニット認証ルール情報受信手段
送信側認証ルール取り出し手段
送信側認証選択手段
送信側認証手段
データ重要性判定手段
受信側認証ルール格納手段
認証ルール情報送信手段
データ
暗号化データ
認証要求
認証
認証ルール関連情報送信
Kw
複数データ認証デジタルAV受信ユニット
単一認証デジタルAVデータ受信ユニット
デジタルAVデータ送信ユニット

【図８】


デジタルＡＶデータ
受信ユニット
92
ＴＶ
認証
Ｄ－Ｉ／Ｆ
91
認証手段
90
認証決定手段
89
管理基準格納手段
88
管理基準参照
決定手段
87
データ重要性
判定手段
86
デジタルＡＶ送信ユニット
93
ＳＴＢ
データ
85

【図９】


デジタルＡＶデータ
受信ユニット
100
ＶＴＲ
機器情報
認証
Ｄ－Ｉ／Ｆ
99
認証手段
98
認証決定手段
97
管理基準格納手段
96
管理基準参照
決定手段
95
ＳＴＢ
94
デジタルＡＶ送信ユニット

【書類名】　要約書

【要約】

【課題】　従来ＡＶデータ装置間のデータの通信では、重要でないデータの認証に多くの時間を要したり、重要なデータであってもその認証が偽造や改竄に弱いという課題がある。

【解決手段】　デジタルＡＶデータの重要度を判定する判定手段３と、複数種類の認証ルールを格納したルール格納手段５と、認証要求を受け、判定手段３の判定結果に基き、ルール格納手段５から一種類のルールを選択する認証選択手段６と、その選択された認証ルールに基づいて認証を行う認証手段７とを有するデジタルＡＶ送信ユニットＳＴＢ１と、認証の要求を行う認証要求手段１２と、ル格納手段５と同じ複数種類の認証ルールを格納したルール格納手段１４と、認証選択手段６で選択された所定の認証ルールと同じ認証ルールを認証ルール格納手段１４から選択する証選択手段１５と、受信側で選択された認証ルールに基づいて認証を行う認証手段１３とを有するデジタルＡＶデータ受信ユニットＴＶ９とを備えたデジタルＡＶデータ送受信システム。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005821
【住所又は居所】　大阪府門真市大字門真１００６番地
【氏名又は名称】　松下電器産業株式会社
【代理人】　申請人
【識別番号】　100092794
【住所又は居所】　大阪市淀川区宮原５丁目１番３号　新大阪生島ビル　松田特許事務所
【氏名又は名称】　松田　正道

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社